

2:18-CR-00292-DWA

The Government applied for court orders to obtain evidence pursuant to 18 U.S.C.A. §§2701-12 of the Electronic Communications Privacy Act (“ECPA”). This portion of the ECPA is commonly referred to as the Stored Communications Act and pertains to stored electronic communications and transaction records by third-party service providers. The Magistrate Judge

granted the Government's applications and certain orders were issued as a result. (ECF No. 318-5, pp. 1-12; No. 318-3, pp. 1-11). Motion to Suppress #10 relates to evidence seized from internet service provider Comcast Communications LLC ("Comcast") for records associated with the email account onedingo@comcast.net from December 15, 2017 to the present. (ECF No. 297/311). Motion to Suppress #11 relates to records seized from internet service provider Tucows¹ associated with the "onedingo.com" domain name and email accounts using the domain name "onedingo.com" from May 2000 to the present.² (ECF No. 298/312).

Pursuant to §2703(c), the Government "may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service... " 18 U.S.C.A. § 2703(c)(1)(B). Disclosure of this type may include the name, address, local and long distance telephone connection records or records of session times and durations, length of service and types of service utilized, telephone / instrument / other subscriber number / identity, and means and source of pay for such service (including any credit card or bank account numbers). 18 U.S.C.A. §2703(c)(2). Such information may be obtained via an order or subpoena. *Id.*

With regard to court orders, §2703(d) provides:

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court ... only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation....

18 U.S.C.A. § 2703 (d). As the Defendant acknowledges, §2703(d) does not require probable cause. (ECF No. 297/311, p. 3, No. 298/312, p. 3). Rather, the "specific and articulable facts"

¹ Tucows refers to Tucows, and its subsidiaries Hover and eNom.

² The Government provides that no records were produced from Tucows in response to the §2703(d) order as to any event history prior to 2011 and as to any archived activity prior to 2013. (ECF No. 352/362, p. 8, n. 2). Thus, there is no information to suppress as it relates to the same. The Defendant does not challenge this. Based on the same, the Defendant's Motion to Suppress No. 11 is denied as moot as it relates to any event history prior to 2011 and as to any archived activity prior to 2013.

standard is derived from the “reasonable suspicion” standard, which is more than a “hunch” but less than both “probable cause” and “a preponderance of the evidence.” See, *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008); *Navarette v. California*, 572 U.S. 393, 397 (2014).³ Furthermore, this standard provides that the information sought is relevant and material to an ongoing criminal investigation and not to a charged offense. In other words, disclosure is proper even if an investigation ultimately does not lead to criminal charges. 18 U.S.C.A. §2703(d).

The Defendant asserts that the records seized from Comcast and associated with the email account, onedingo@comcast.net, should be suppressed because: 1) the Application for the order relied on ill-gotten evidence, and absent that evidence, the Application failed to establish reasonable grounds to believe the same are relevant and material to an ongoing criminal investigation, and 2) regardless, the Application failed to establish reasonable grounds for the relevance and materiality of the records sought. (ECF No. 297/311). The Defendant further seeks to suppress evidence seized from Tucows for records associated with “onedingo.com,” a domain name, and all email accounts using the domain name “ondingo.com,” because the Order was overbroad. (ECF No. 298/312).

The pertinent Applications have been provided for review. Upon review, I find that the Government provided “specific and articulable facts” showing there are reasonable grounds to believe that the information sought is relevant and material to the ongoing criminal investigation. See, *Application of the United States For An Order Pursuant to* 18 U.S.C. § 2703(d). (ECF No. 318-3, pp. 1-6; and No. 318-5, pp. 1-7). Based on the information contained in the Applications, there were reasonable grounds for the Magistrate Judge to believe that the information sought could be relevant and material to the ongoing criminal investigation, including information related

³ The Defendant cites to *United States v. Stearn*, 597 F.3d 540, 560 (3d Cir. 2010), for the proposition that the Government must show a direct nexus between or connection to the place to be searched and the crime under investigation. (ECF No. 298/312, p. 3). *Stearn*, however, does not discuss the “specific and articulable facts” showing “reasonable grounds to believe” standard of the ECPA case and only relates to search warrants. As a result, I find *Stearn* is not applicable here.

to racial animus, planning and premeditation, and/or information relevant to the §247 offense being investigated, which has an element that the offense was committed in or affecting interstate commerce.

Additionally, as to Motion to Suppress No. 11, I do not find the order granting the Government's Application was overbroad. Specifically, the Application established that Tucows account onedingo.com and email addresses were controlled by the Defendant since May 2000 and that the Defendant used social media and email as a means to communicate bias against Jewish people with the public and with his relatives. (ECF No. 318-3, pp. 1-6). Therefore, I find it was reasonable to believe that the information sought from Tucows could be relevant and material to the ongoing investigation.⁴ Thus, based on the above, I further find the Application associated with Motion to Suppress No. 10 did not rely on illegally obtained evidence related to the Tucows Order as the basis for seeking records associated with onedingo@comcast.net.⁵

Regardless, even if reasonable grounds to believe the information sought is relevant and material to an ongoing investigation as to both Orders is lacking, suppression is not the appropriate remedy. 18 U.S.C.A. §2707-08; *See also, United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008).

[S]ection 2708 of the ECPA specifically states that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Section 2707, in turn, describes remedies for violations of the Act as including civil actions for violators other than the United States and administrative discipline against federal employees in certain circumstances. 18 U.S.C. § 2707. Thus, violations of the

⁴ Again, I note the Government states that Tucows produced no records in response to the §2703(d) order as to any event history prior to 2011 and as to any archived activity prior to 2013. (ECF No. 352/362, p. 8, n. 2). Thus, there is no information to suppress as it relates to the same. The Defendant does not challenge this. Based on the same, the Defendant's Motion to Suppress No. 11 is denied as moot as it relates to any event history prior to 2011 and as to any archived activity prior to 2013.

⁵ Additionally, as the Government points out, it had independent evidence that the onedingo@comcast.net email was controlled by the Defendant. "Even if the Tucows response had been limited to providing the email address associated with the account as of 'six months before October 27, 2018,' the time frame that the defendant concedes was relevant to the ongoing investigation, Doc. No. 297 at 4, the end result would have been the same: Tucows would have reported that the email address was onedingo@comcast.net and the government would have received the same IP history which only dated back to July 2018." (ECF No. 352/362, pp. 10-11, n.4). The Defendant does not contest this assertion.

ECPA do not warrant exclusion of evidence. See *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir.2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir.1998); *Bansal v. Russ*, 513 F.Supp.2d 264, 282–83 (E.D.Pa.2007); *United States v. Sherr*, 400 F.Supp.2d 843, 848 (D.Md.2005); *United States v. Kennedy*, 81 F.Supp.2d 1103, 1110 (D.Kan.2000).

Perrine, 518 F.3d at 1202 (10th Cir. 2008). Therefore, suppression of the evidence obtained is not the appropriate remedy pursuant to the ECPA unless there is a constitutional violation.

To that end, I do not find the Fourth Amendment is applicable to the ECPA Orders as Defendant seems to be suggesting. See, *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010), citing *Perrine*, 518 F.3d at 1204-05 (collecting cases)(“Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”). The Defendant does not assert a privacy interest in the non-content subscriber information maintained by third parties (Comcast and Tucows) such as the information at issue here and has cited no cases law or argument to support a privacy interest in said information. See, ECF Nos. 297/311, 298/312. Consequently, I find the Fourth Amended is not implicated and, thus, suppression pursuant to the Fourth Amendment is not warranted as to the information challenged in the Defendant’s Motions to Suppress Nos. 10 and 11. Accordingly, the Defendant’s Motions to Suppress Nos. 10 and 11 are denied.

An appropriate order shall follow.

